TOO GOOD TO BE TRUE....

A Column on Consumer Issues by Attorney General Wayne Stenehjem's Consumer Protection and Antitrust Division

August 13, 2003

"Phishing" Scam

When Internet scammers go casting about for people's financial information, "phishing" (pronounced fishing) is one of the newest ways unsuspecting victims can be lured. Phishing, also called "carding," is a high-tech scam that uses spam to deceive consumers into disclosing their credit-card numbers, bank-account information, social security numbers, passwords, and other sensitive information.

Here's how it works. The consumer receives an e-mail that claims to be from businesses the potential victim deals with – such as their Internet service provider, online payment service or bank. The fraudsters tell the consumers they need to "update" or "validate" their billing information to keep their accounts active, and direct them to a "look-alike" website of the legitimate business, further tricking consumers into thinking they are responding to a *bona fide* request. Unknowingly, consumers submit their financial information – not to the businesses – but to the scammers, who use it to order goods and services and obtain credit. The consumer has just become a victim of identity theft.

To avoid getting caught by these scams, here are some guidelines to follow:

- If you get an e-mail that warns you, with little or no notice, that an account of yours will be shut down unless you reconfirm you billing information, do not reply or click on the link in the e-mail. Instead, contact the company cited in the e-mail using the telephone number or website address you know to be genuine

- Avoid e-mailing personal and financial information. Before submitting financial information through a website, look for the "lock" icon on the browser's status bar. It signals that your information is secure during transmission.

- Review credit card and bank account statements as soon as you receive them to determine whether there are any unauthorized charges. If your statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances.

- Report suspicious activity to the Federal Trade Commission. Send the actual spam to use@ftc.gov. If you believe you've been scammed, file your complaint at www.ftc.gov, and then visit the FTC's Identity Theft website (www.ftc.gov/idtheft) to learn how to minimize your risk of damage from identity theft.

Recent phishing scams cleverly copied the web pages of well-known Internet companies like E-Bay, Pay-Pal, and Earthlink. Using these authentic looking but fake web pages, they then collected personal information from Internet consumers, who thought they were visiting the real E-Bay, Pay-Pal or Earthlink.

The Attorney General's Consumer Protection Division investigates allegations of fraud in the marketplace. Investigators also mediate individual complaints against businesses. If you have a consumer problem or question, call the Consumer Protection Division at 328-3404, toll-free at 1-800-472-2600, or 1-800-366-6888 (w/TTY). This article and other consumer information is located on our website at www.ag.state.nd.us.

*** * * * ***